Axalto, Inc
8311 North FM 620 Rd
Austin, TX, 78726

November 10th, 2004.

Arthur K. Wu,
Staff Director, Subcommittee on Oversight and Investigations
Room 337A, Cannon House Office Building
Washington DC 20515

Dear Mr. Wu,

With regard to the five (5) questions received from Chairman Buyer since the Hearing on Oct 6th, I have detailed my answers below.

Q1 : **In your Opinion, is the VA model of identification easily applicable to other Federal agencies and departments?**

A1 : The use of smart cards in an identity management system provides many benefits. The VA implementation is making good use of combining both the physical and logical identification credentials onto one common identification smart ID card that is intended to work at all equipped VA locations. With the recent publication of HSPD-12 there is now a heightened sense of urgency for all Federal agencies to put credentialing programs in place. NIST has been tasked to create a new FIPS PUB (FIPS PUB 201) that details the implementation specification. At present the document is in early draft and is drawing from the vast experiences that exists in Federal agencies whom have already deployed or who are in the process of deploying credentialing systems using smart cards. The VA system is one example of an Identity Management system which can have significant influence on the future FIPS PUB 201 as well as facilitate other Federal agencies to save time from the well directed investments made to date on the VA program.

Q2 : **What Problems do you foresee in extending the smart card initiative to Federal agencies and departments that are in the beginning stages such as Social Security and HUD?**

A2 : *Each Federal agency has many pre-existing issues that may turn out to be constraints or opportunities when deploying an Identity Management system. Some of these issues include existing contracts, budget constraints and cultures that may not understand or embrace the technology. Each Federal agency must implement an identity management system that matches their needs taking into account their existing infrastructure and operational process whilst making sure it is interoperable with other agency identity management systems. Clearly a comprehensive specification is needed that covers the main important areas for ensuring interoperability in between Federal agencies. This is now the role of HSPD-12 and FIPS PUB 201.*

Q3 : **Is the idea of a smart card a conceivable option for all citizens as a general form of identification?**

A3 : *A smart card can serve as the local security agent of the Issuer (e.g. Federal or State Government etc) in the hands of the card holder (e.g. Citizen). With proven high levels of card holder identity authentication the smart card can be a valuable asset in verifying a person's* *identity back to a reference credential they supplied when they enrolled into the system. In the event that the Federal or State Government wish to address the weak security of existing general forms of identification, smart card technology, in combination with other security technologies can be used to form a much stronger and trusted form of general identification. The smart card can also protect the privacy of the card holder by limiting access to information based on the access rights of the requestor and only when authorized by the card holder.*

Q4 **: Using the guidelines issued under HSPD-12, is a future national database conceivable/desirable?**

A4 : *HSPD-12 defines a "Policy for a Common Identification Standard for Federal Employees and Contractors". As such HSPD-12 instructs each Federal agency to have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the new Standard. It does not mention anything regarding a future national database. As each Federal agency has the responsibility for protecting their employee's privacy it is unnecessary for a national identity or credential database.*

Q5 : **How would individual's right to privacy and protection of liberties be guaranteed?**

A5 : *Smart card technology is able to protect information assets by ensuring that access to information are limited to authorized requestors and data divulgence can be made subject to the card holders consent. Smart Cards can also perform biometric comparisons within the card itself meaning that the enrollment biometric never leaves the card when live captured biometrics are set into the card for matching.*

Yours Sincerely

Neville Pattinson